PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 21 July 1999 (21.07.99)	
International application No. PCT/US98/26069	**Applicant's or agent's file reference** RCA 88783
International filing date (day/month/year) 09 December 1998 (09.12.98)	**Priority date** (day/month/year) 10 December 1997 (10.12.97)
Applicant ESKICIOGLU, Ahmet, Mursit et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

17 June 1999 (17.06.99)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Jocelyne Rey-Millet

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
RCA 88783		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US 98/ 26069	09/12/1998	10/12/1997
Applicant		
THOMSON CONSUMER ELECTRONICS, INC. et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. [ ] **Certain claims were found unsearchable** (see Box I).

2. [ ] **Unity of invention is lacking** (see Box II).

3. [ ] The international application contains disclosure of a **nucleotide and/or amino acid sequence listing** and the international search was carried out on the basis of the sequence listing
   - [ ] filed with the international application.
   - [ ] furnished by the applicant separately from the international application,
     - [ ] but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.
   - [ ] Transcribed by this Authority

4. With regard to the **title,**
   - [X] the text is approved as submitted by the applicant
   - [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   - [X] the text is approved as submitted by the applicant
   - [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this International Search Report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is:
   Figure No. 2
   - [X] as suggested by the applicant.
   - [ ] because the applicant failed to suggest a figure.
   - [ ] because this figure better characterizes the invention.
   - [ ] None of the figures.

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

TRIPOLI, Joseph, S.
Thomson Multimedia Licensing Inc.
P.O. Box 5312
Princeton, NJ 08540
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Rule 71.1)

Date of mailing *(day/month/year)*	25. 02. 00
Applicant's or agent's file reference RCA 88783	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US98/26069	09/12/1998	10/12/1997

Applicant
THOMSON CONSUMER ELECTRONICS, INC. et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Stannartz, B Tel.+49 89 2399-8242

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
RCA 88783		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US98/26069	09/12/1998	10/12/1997
International Patent Classification (IPC) or national classification and IPC H04N7/16		
Applicant THOMSON CONSUMER ELECTRONICS, INC. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
17/06/1999	25. 02. 00
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Luckett, P Telephone No. +49 89 2399 8965

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US98/26069

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

2-7	as originally filed	
1	with telefax of	09/12/1999

Claims, No.:

8	as originally filed	
1-7	with telefax of	09/12/1999

Drawings, sheets:

1/3-3/3	as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-8
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-8
Industrial applicability (IA)	Yes:	Claims	1-8
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 The subject matter of the claims lacks an inventive step having regard to the disclosure of:-

D1: EP-A-0 658 054 (NEWS DATACOM LTD) 14 June 1995 ; and
D2: CHAMBERS W G: 'SOLUTION OF WELCH-BERLEKAMP KEY EQUATION BY EUCLIDEAN ALGORITHM' ELECTRONICS LETTERS, vol. 29, no. 11, 27 May 1993, page 1031 XP000372940

2 D1 discloses a conditional access system for use with a network including a transmitter and a multiplicity of receivers, each receiver being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, each of the multiplicity of receivers including: a first key generator, **employing at least part of the data and a function** which differs for at least a plurality of ones of the multiplicity of receivers, for generating a **first key which is different for each receiver** having **a different function**, a second key generator employing at least part of the data and the function to produce a second key, and a secret number generator utilizing the first key with the second key to produce the secret number which is the same for all of the multiplicity of receivers, whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function.

3 All features of amended claim 1 are known from the citation D1, with the sole exception that (as defined in feature (c) of the claim) "said second value being **pre**-stored in said smart card" (emphasis added). In D1 and "algorithm" is used (see D1 col 6, lines 16-20) to generate one of two keys ("seed3" and "delta3") used to descramble the received signals. While D1 does not explicitly mention the use of a stored constant value in this algorithm which would read onto the sole distinguishing feature of claim 1 and thereby fully anticipating the claim's subject matter, it is hardly conceivable that any appropriate algorithm might not involve such a value (or defacto effective second key). In any event the provision of such

an element in the algorithm of D1 is regarded to be a mere matter of routine design normally to be expected of a skilled person.

4 The further specification that the second value is **pre**-stored in the smart card can have no real technically limiting effect upon the claim scope. This is because no time frame is defined in the claim w.r.t. the act of storing the second value, which could exclude the interpretation that the **pre**-stored value was simply derived from an earlier part of the respective signal transmission.

4 Claims 2-4 define only matters of routine design for a skilled person and thus also lack inventive step. In particular the features of points in a "Euclidean plane" and "calculation of the Y intercept" for generation of decoding keys is a known technique in this technical field as demonstrated by the disclosure of D2. The polynomial used in the embodiments of the present application relate to first order linear functions with minimum computational requirement and are thus the very first functions which a skilled person would inevitably consider using. Similar objection applies to the subject matter of claims 5-8.

PATENT COOPERATION TREATY

REC'D 29 FEB 2000
WIPO PCT

PCT

16

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
RCA 88783		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US98/26069	09/12/1998	10/12/1997
International Patent Classification (IPC) or national classification and IPC H04N7/16		
Applicant THOMSON CONSUMER ELECTRONICS, INC. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
17/06/1999	25.02.00
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Luckett, P Telephone No. +49 89 2399 8965

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US98/26069

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

2-7	as originally filed	
1	with telefax of	09/12/1999

Claims, No.:

8	as originally filed	
1-7	with telefax of	09/12/1999

Drawings, sheets:

1/3-3/3	as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-8
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-8
Industrial applicability (IA)	Yes:	Claims	1-8
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 The subject matter of the claims lacks an inventive step having regard to the disclosure of:-

D1: EP-A-0 658 054 (NEWS DATACOM LTD) 14 June 1995 ; and
D2: CHAMBERS W G: 'SOLUTION OF WELCH-BERLEKAMP KEY EQUATION BY EUCLIDEAN ALGORITHM' ELECTRONICS LETTERS, vol. 29, no. 11, 27 May 1993, page 1031 XP000372940

2 D1 discloses a conditional access system for use with a network including a transmitter and a multiplicity of receivers, each receiver being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, each of the multiplicity of receivers including: a first key generator, **employing at least part of the data and a function** which differs for at least a plurality of ones of the multiplicity of receivers, for generating a **first key which is different for each receiver** having **a different function**, a second key generator employing at least part of the data and the function to produce a second key, and a secret number generator utilizing the first key with the second key to produce the secret number which is the same for all of the multiplicity of receivers, whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function.

3 All features of amended claim 1 are known from the citation D1, with the sole exception that (as defined in feature (c) of the claim) "said second value being **pre**-stored in said smart card" (emphasis added). In D1 and "algorithm" is used (see D1 col 6, lines 16-20) to generate one of two keys ("seed3" and "delta3") used to descramble the received signals. While D1 does not explicitly mention the use of a stored constant value in this algorithm which would read onto the sole distinguishing feature of claim 1 and thereby fully anticipating the claim's subject matter, it is hardly conceivable that any appropriate algorithm might not involve such a value (or defacto effective second key). In any event the provision of such

an element in the algorithm of D1 is regarded to be a mere matter of routine design normally to be expected of a skilled person.

4 The further specification that the second value is **pre**-stored in the smart card can have no real technically limiting effect upon the claim scope. This is because no time frame is defined in the claim w.r.t. the act of storing the second value, which could exclude the interpretation that the **pre**-stored value was simply derived from an earlier part of the respective signal transmission.

5 Claims 2-4 define only matters of routine design for a skilled person and thus also lack inventive step. In particular the features of points in a "Euclidean plane" and "calculation of the Y intercept" for generation of decoding keys is a known technique in this technical field as demonstrated by the disclosure of D2. The polynomial used in the embodiments of the present application relate to first order linear functions with minimum computational requirement and are thus the very first functions which a skilled person would inevitably consider using. Similar objection applies to the subject matter of claims 5-8.

RCA 88783

CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS

Field of the Invention

This invention concerns a system for providing conditional access (i.e., managing access) to a received scrambled audio/visual (A/V) signal from a variety of sources, such as, broadcast television networks, cable television networks, digital satellite systems, and internet service providers. Utilizing the concept of secret sharing, the system does not require full descrambling keys to be sent to the receiving device under encryption. The keys are recovered using a seed value received from the service provider and a seed value stored in the device.

Background of the Invention

Today, a user may receive services from a variety of service providers, such as broadcast television networks, cable television networks, digital satellite systems, and internet service providers. Most television receivers are capable of receiving unscrambled information or programs directly from broadcast and cable networks. Cable networks providing scrambled (or encrypted) programs usually require a separate stand alone set-top box to descramble (or decrypt) the program. Similarly, digital satellite systems usually provide scrambled programs that also require the use of a separate set-top box. These set-top boxes may utilize a removable smart card which contain the keys necessary for recovering the scrambling or descrambling keys. Protection of these important keys is paramount to prevent unauthorized copying of the programming.

European Patent Application Number EP-A-0 658 054 discloses generating a descrambling key using two pieces of transmitted data.

Summary of the Invention

In a conditional access (CA) system, the signals are usually scrambled using symmetric ciphers such as the Data Encryption Standard (DES). For security reasons, the scrambling key is

AMENDED SHEET

Claims

1. A method for managing access to a signal representative of an event of a service provider, said method comprising:

(a) receiving said signal in a smart card, said signal being scrambled using a scrambling key;

(b) receiving, in said smart card, data representative of a first seed value;

characterized in that

(c) generating said scrambling key using said first seed value and a second seed value, said second seed value being pre-stored in said smart card; and

(d) descrambling said signal using said generated scrambling key to provide a descrambled signal.

2. The method of Claim 1 wherein said first and second seed values are points on a Euclidean plane.

3. The method of Claim 2 wherein the step of generating said scrambling key comprises calculating the Y-intercept of a line formed on said Euclidean plane by said first and second seed values.

4. The method of Claim 3 wherein said smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMCIA card standards.

5. In combination in a system for managing access between a service provider and a device having a smart card coupled thereto, said device performing the steps of:

(a) receiving from the service provider a signal representative of an event, said signal being scrambled using a scrambling key;

(b) receiving from the service provider data representative of a first seed value, said first seed value being selected from a Euclidean plane; characterized in that

(c) coupling said scrambled signal and said first seed value to said smart card, said smart card having a means for access control processing; said access control processing means comprising means for generating said scrambling key by calculating the Y-intercept of a line on said Euclidean plane by said first seed value and a second seed value, said second seed value being pre-stored in said smart card and means for descrambling said signal using said generated scrambling key to generate a descrambled signal; and

(d) receiving from said smart card said descrambled signal.

6. The combination of Claim 5 wherein the device is a set-top box.

7. The combination of Claim 5 wherein the device is a digital television.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/16 — A1

(11) International Publication Number: WO 99/30498

(43) International Publication Date: 17 June 1999 (17.06.99)

(21) International Application Number: PCT/US98/26069

(22) International Filing Date: 9 December 1998 (09.12.98)

(30) Priority Data:
60/069,063 10 December 1997 (10.12.97) US

(71) Applicant *(for all designated States except US)*: THOMSON CONSUMER ELECTRONICS, INC. [US/US]; 10330 North Meridian Street, Indianapolis, IN 46290–1024 (US).

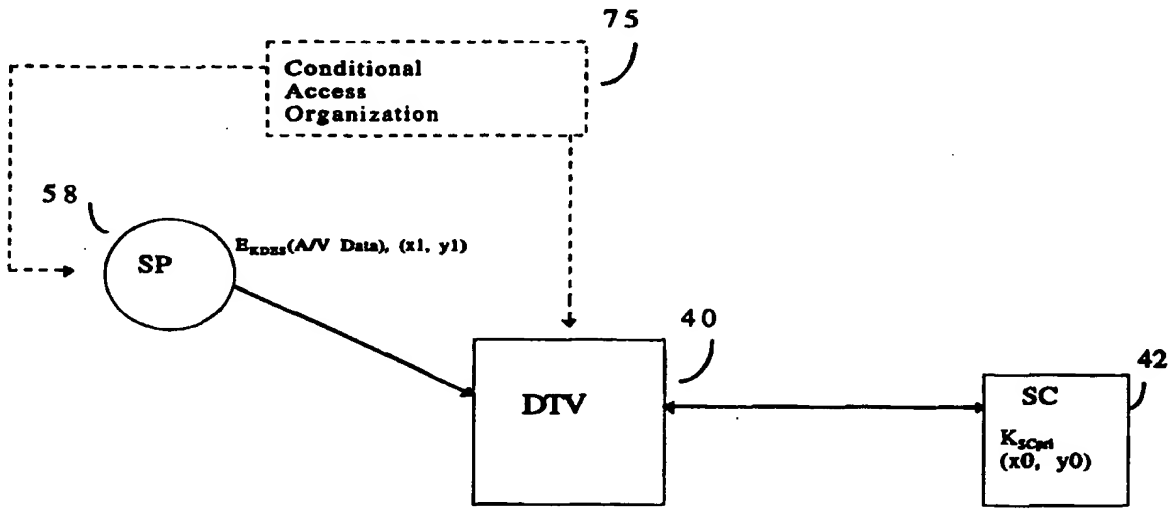
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ESKICIOGLU, Ahmet, Mursit [TR/US]; 8235 Lakeshore Trail #125, Indianapolis, IN 46250 (US). OZKAN, Mehmet, Kemal [TR/TR]; Savasci Sokak Bozokatt 19/1, Avcilar, 34840 Istanbul (TR). BEYERS, Billy, Wesley, Jr. [US/US]; 6920 Woodcrest Drive, Greenfield, IN 46104 (US).

(74) Agents: TRIPOLI, Joseph, S. et al.; GE & RCA Licensing Management Operation, Inc., P.O. Box 5312, Princeton, NJ 08540 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS



(57) Abstract

A method for providing conditional access (i.e., managing access) to a received scrambled audio/visual (A/V) signal from a variety of sources by utilizing secret sharing for key recovery. Secret sharing eliminates the necessity to protect and transfer the complete descrambling keys between devices, because a portion of the key is stored in the device or a smart card coupled thereto.

CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS

Field of the Invention

This invention concerns a system for providing conditional access (i.e., managing access) to a received scrambled audio/visual (A/V) signal from a variety of sources, such as, broadcast television networks, cable television networks, digital satellite systems, and internet service providers. Utilizing the concept of secret sharing, the system does not require full descrambling keys to be sent to the receiving device under encryption. The keys are recovered using a seed value received from the service provider and a seed value stored in the device.

Background of the Invention

Today, a user may receive services from a variety of service providers, such as broadcast television networks, cable television networks, digital satellite systems, and internet service providers. Most television receivers are capable of receiving unscrambled information or programs directly from broadcast and cable networks. Cable networks providing scrambled (or encrypted) programs usually require a separate stand alone set-top box to descramble (or decrypt) the program. Similarly, digital satellite systems usually provide scrambled programs that also require the use of a separate set-top box. These set-top boxes may utilize a removable smart card which contain the keys necessary for recovering the scrambling or descrambling keys. Protection of these important keys is paramount to prevent unauthorized copying of the programming.

Summary of the Invention

In a conditional access (CA) system, the signals are usually scrambled using symmetric ciphers such as the Data Encryption Standard (DES). For security reasons, the scrambling key is

changed frequently, the period of change being as frequent as every few seconds. The protection of the descrambling keys, which need to be sent with the signals, is often provided by public-key cryptography. Public-key cryptography introduces problems associated with the public key infrastructure and distribution of the keys. This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem.

A signal (e.g., an event or program) as described herein comprises information such as (1) audio/visual data (for example, a movie, weekly "television" show or a documentary); (2) textual data (for example, an electronic magazine, paper, or weather news); (3) computer software; (4) binary data (for example, images); (5) HTML data (for example, web pages); or any other information for which access control may be involved. The service providers include any provider broadcasting events, for example, traditional broadcast television networks, cable networks, digital satellite networks, providers of electronic list of events, such as electronic program guide providers, and in certain cases internet service providers.

Generally, the present invention defines a method for managing access to a signal, representative of an event of a service provider, utilizing a smart card. That is, this method comprises receiving in a smart card, a signal that is scrambled using a scrambling key, receiving data representative of a first seed value, generating the scrambling key using the first seed value and a second seed value that is stored in the smart card and descrambling the signal using the generated scrambling key to provide a descrambled signal.

In accordance with one aspect of the present invention, the first and second seed values are points on a Euclidean plane and the step of generating the scrambling key comprises calculating

the Y-intercept of the line formed on the Euclidean plane by the first and second seed values.

In accordance with still another aspect of the present invention, a system for managing access between a service provider and a device having a smart card coupled to the device involves the device performing the steps of receiving from the service provider a signal representative of an event that is scrambled using a scrambling key, receiving from the service provider data representative of a first seed value selected from a Euclidean plane, and coupling the scrambled signal and the first seed value to the smart card. The smart card has a means for access control processing comprising means for generating a scrambling key by calculating the Y-intercept of the line formed in the Euclidean plane by the first seed value and a second seed value stored in the smart card and means for descrambling the signal using the generated scrambling key to generate a descrambled signal.

These and other aspects of the invention will be explained with reference to a preferred embodiment of the invention shown in the accompanying Drawings.

Brief Description of the Drawing

Figure 1 is a block diagram illustrating one architecture for interfacing a common set-top box to a variety of service providers.

Figure 2 is a block diagram of an exemplary implementation of a system for managing access to a device in accordance with the invention;

Figure 3a is a graphical representation of the determination of the scrambling key in accordance with one embodiment of this invention; and

Figure 3b is a graphical representation of an allocation of a unique and non-overlapping range for each service provider in accordance with Figure 3a.

Detailed Description of the Drawing

The present invention provides a conditional access system which may be utilized to obtain services from one of a plurality of sources. The conditional access system when implemented within a device, such as a digital television, digital video cassette recorder or set-top box, provides convenient management of the descrambling keys because only a portion of the seed value necessary for key generation is stored therein. For simplicity, the below description of the invention will be directed towards an implementation using a digital television and a smart card.

In Figure 1, system 30 depicts the general architecture for managing access to a digital television (DTV) 40. Smart Card (SC) 42 is inserted into, or coupled to, a smart card reader 43 of DTV 40; an internal bus 45 interconnects DTV 40 and SC 42 thereby permitting the transfer of data therebetween. Such smart cards include ISO 7816 cards having a card body with a plurality of terminals arranged on a surface in compliance with National Renewable Security Standard (NRSS) Part A or PCMCIA cards complying with NRSS Part B. Conceptually, when such a smart card is coupled to a smart card reader, the functionality of the smart card may be considered to be a part of the functionality of the device (e.g., DTV 40) thus removing the "boundaries" created by the physical card body of the smart card.

DTV 40 can receive services from a plurality of service providers (SPs), such as a broadcast television SP 50, a cable television SP 52, a satellite system SP 54, and an internet SP 56. Conditional Access Organization (CA) 75 is not directly connected to either the service providers or STB 40 but deals with key

management and issues public and private key pairs which may be used, if necessary, as explained below.

The present invention employs the concept of secret sharing which eliminates the requirement for using public key cryptography to ensure secure transmission of the audio/visual (A/V) stream from a service provider. A variation of a secret sharing scheme, developed by Adi Shamir, is known as a threshold scheme. An (m, n) threshold scheme involves breaking a secret into n pieces (which may be called shadows), in such a way that at least m (<=n) of the pieces are required to reconstruct the secret. A perfect threshold scheme is a threshold scheme in which a knowledge of m-1 or fewer shadows provides no information about the secret. For example, with a (3,4)-threshold scheme, the secret is divided into four portions but only three of the four portions are required to reconstruct the secret. Two of the portions, however, cannot reconstruct the secret. In Shamir's (m, m) threshold scheme, choosing a higher value for m, and storing (m-1) secrets in the card would increase the system's resistance to ciphertext only attacks, but would lead to more computations for polynomial construction.

Such a threshold scheme reduces the computational requirements for the card in DES key recovery. For each new key, only a simple operation is performed (i.e., the value of the polynomial at x = 0 is computed) as compared to RSA decryption which involves modular exponentiation. Additionally, security is "perfect" (i.e., given knowledge of (x_1, y_1), all values of the secret remain equally probable).

Figures 2 and 3 together, demonstrate one embodiment of the present invention. Particularly, stored in SC 42 is a first seed value (or data point). The first seed value may be thought of as a single point on a Euclidean plane, i.e., in the form of (x0, y0). Service provider 58 transmits a signal (or event or program) that may be scrambled by a symmetric key, for example a Data Encryption Standard (DES) key. In addition to the scrambled

signal, service provider 58 transmits a second seed value. Similarly, the second seed value may be a second single point from the same Euclidean plane, i.e., in the form of (x1, y1).

The scrambled A/V signal and the second seed value is received by DTV 40 and is coupled to SC 42 for processing. SC 42 receives the second seed value and utilizes both the stored first seed value and the received second seed value to reconstruct (or recover) the symmetric key. SC 42 uses the reconstructed symmetric key to descramble the received scrambled A/V signal and generate a descrambled A/V signal. This descrambled A/V signal is provided to DTV 40 for display.

Recovery of the symmetric key is achieved by constructing a polynomial utilizing the first and the second seed values; the y-intercept of the constructed polynomial is the symmetric key. For example, given (x0, y0) and (x1, y1), the symmetric key is constructed by computing the value of $[\{(y1-y0)/(x1-x0)\}(x-x0)] + y0$ at $x = 0$. Figure 3a illustrates a graphical representation of the present invention.

Such an approach permits more than one service provider to share the stored second seed value (x0, y0). Each service provider would then be free to choose its own first seed value. The probability of constructing polynomials with identical y-intercepts (i.e., identical symmetric keys) is low. However, the range of possible second seed values could be allocated such that each service provider has a unique and non-overlapping range (see Figure 3b). Further, it is within the scope of the present invention that each service provider could choose its own first seed value which could be encrypted using the public key of the smart card before downloading. The seed value would be recovered by the smart card using its stored private key (K_{SCpri}).

The general architecture of system 30 lends itself to achieving the goal of minimizing the amount of information (or

keys) that needs to be stored in a smart card to permit access to more than one service provider.

The robustness of the defined system may be increased by scrambling portions of the event with different keys and transmitting different second seed values. Further, it is within the scope of the present invention that more than two seed values may be used to recover the symmetric key. For example, two or more seed value may be stored in the smart card and a seed value may be transmitted with the encrypted A/V signal. The symmetric key would be recovered using all of the seed values.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in the art and it is intended to include such alterations within the scope of the appended claims.

Claims

1. A method for managing access to a signal representative of an event of a service provider, said method comprising:

(a) receiving said signal in a smart card, said signal being scrambled using a scrambling key;

(b) receiving, in said smart card, data representative of a first seed value;

(c) generating said scrambling key using said first seed value and a second seed value, said second seed value being stored in said smart card; and

(d) descrambling said signal using said generated scrambling key to provide a descrambled signal.

2. The method of Claim 1 wherein said first and second seed values are points on a Euclidean plane.

3. The method of Claim 2 wherein the step of generating said scrambling key comprises calculating the Y-intercept of a line formed on said Euclidean plane by said first and second seed values.

4. The method of Claim 3 wherein said smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMCIA card standards.

5. In combination in a system for managing access between a service provider and a device having a smart card coupled thereto, said device performing the steps of:

(a) receiving from the service provider a signal representative of an event, said signal being scrambled using a scrambling key;

(b) receiving from the service provider data representative of a first seed value, said first seed value being selected from a Euclidean plane;

(c) coupling said scrambled signal and said first seed value to said smart card, said smart card having a means for access control processing;

said access control processing means comprising means for generating said scrambling key by calculating the Y-intercept of a line on said Euclidean plane by said first seed value and a second seed value, said second seed value being stored in said smart card and means for descrambling said signal using said generated scrambling key to generate a descrambled signal; and

(d) receiving from said smart card said descrambled signal.

6. The combination of Claim 5 wherein the device is a set-top box.

7. The combination of Claim 5 wherein the device is a digital television.

8. The combination of Claim 5 wherein the device is a digital video cassette recorder.

09/581064
PCT/US98/26069

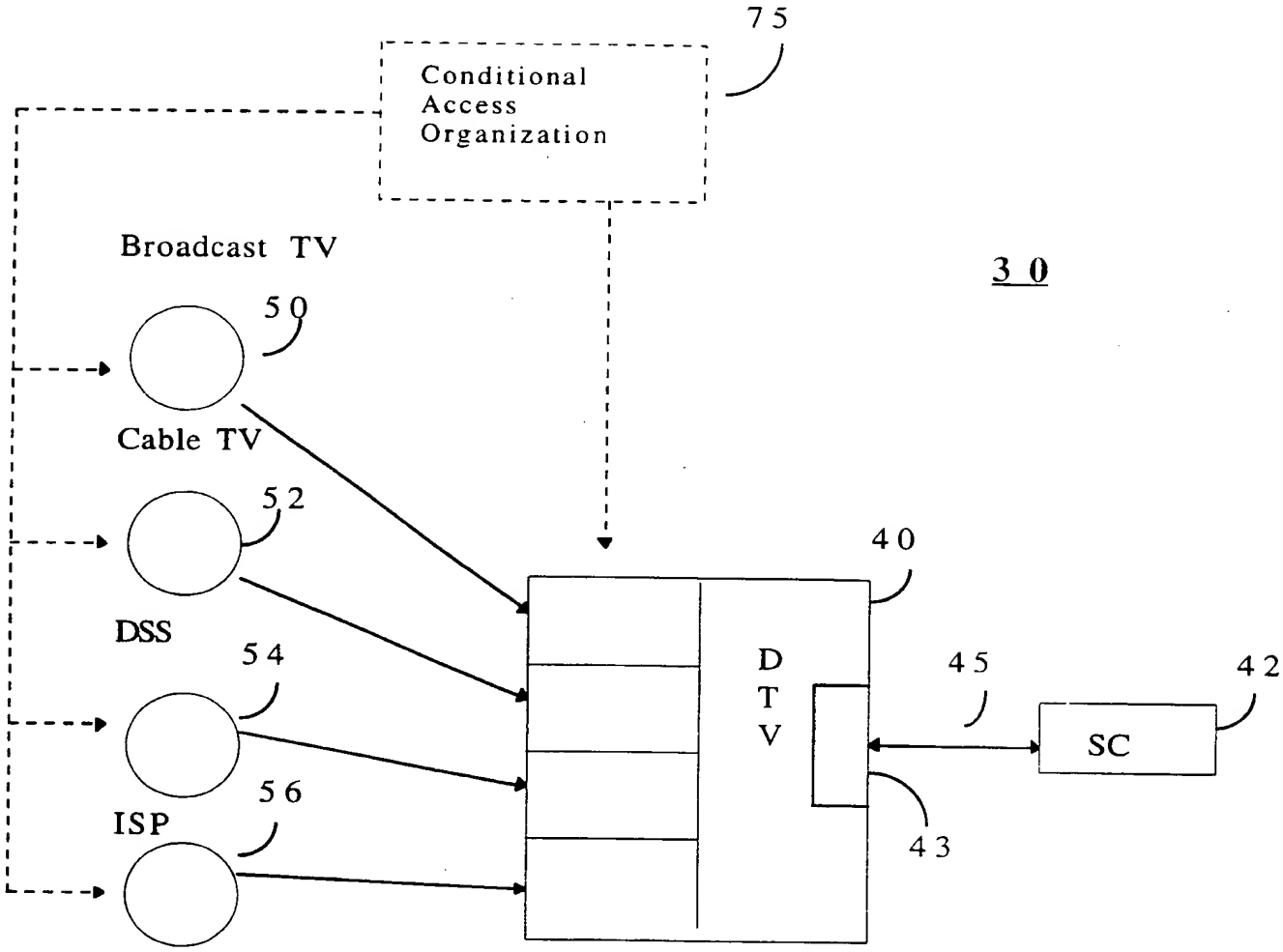


Fig. 1

09/581064

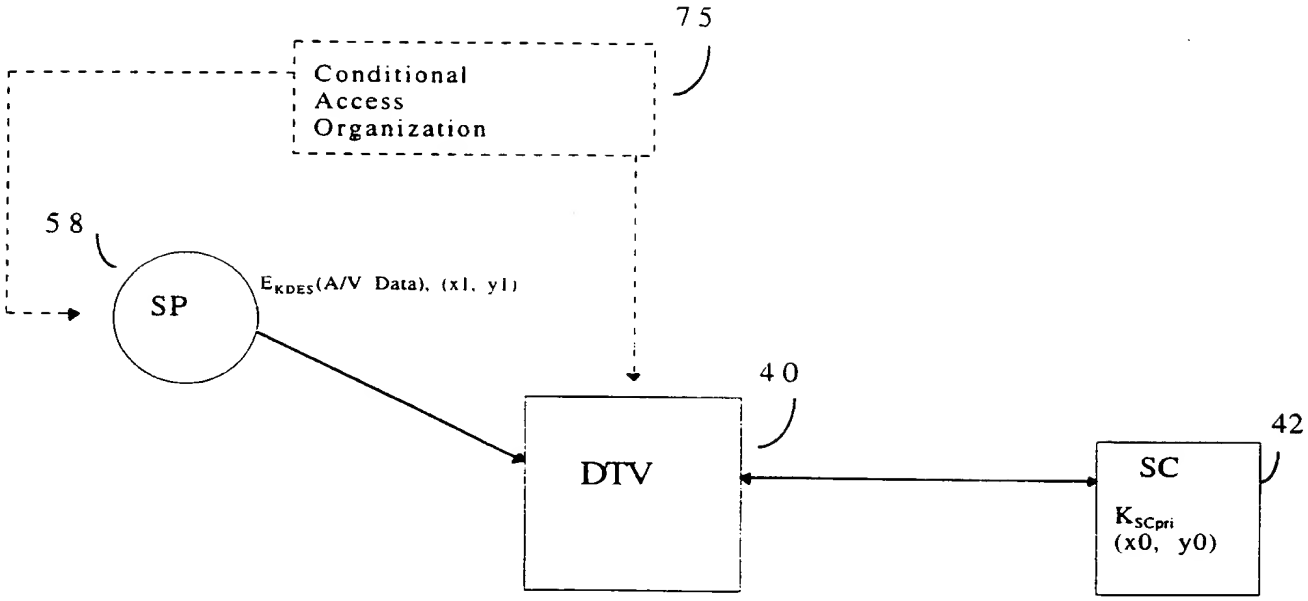


Fig. 2

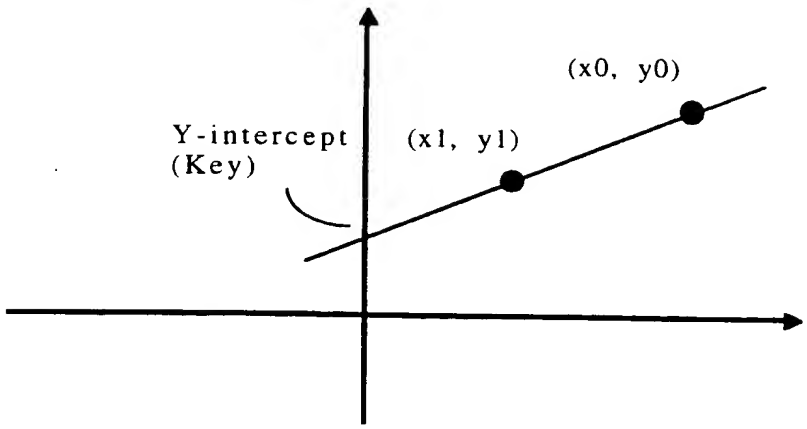


Fig. 3a

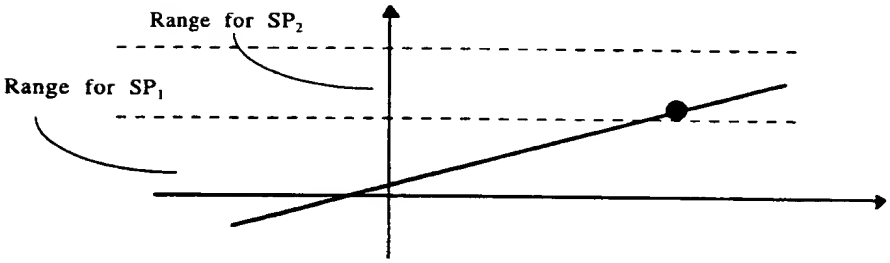


Fig. 3b

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.